Publicado en Madrid el 14/03/2019

Más de 200 aplicaciones de Google Play infectadas por la vulnerabilidad SimBad

Desde Check Point señalan el bajo nivel de protección que muestran las empresas, ya que el 59% no ha implementado soluciones de seguridad móvil

Check Point® Software Technologies Ltd. (NASDAQ: CHKP), proveedor líder especializado en ciberseguridad a nivel mundial, ha encontrado una vulnerabilidad en 206 aplicaciones de Google Play Store, las cuales cuentan con cerca de 150 millones de descargas. Conocida como 'SimBad' debido a que la mayoría de las aplicaciones infectadas son simuladores (juegos), esta vulnerabilidad provoca una campaña masiva de adware móvil por medio del cual se muestran innumerables anuncios fuera de la aplicación sin que exista posibilidad de desinstalar dichas aplicaciones.

"Los dispositivos móviles se están convirtiendo en los últimos tiempos en el principal foco de los ataques de los ciberdelicuentes. Casi 6 de cada 10 empresas no han implementado soluciones de seguridad móvil capaces de detectar amenazas como el malware móvil, aplicaciones falsas o maliciosas, ataques man-in-the-middle y vulnerabilidades de sistema", señala Eusebio Nieva, director técnico de Check Point para España y Portugal. "Estos datos ponen de manifiesto la necesidad que tienen las empresas para poder proteger sus dispositivos ante amenazas de este tipo", añade Nieva.

¿Cómo funciona SimBad?

Las actividades que SimBad puede desarrollar se dividen en 3 grupos: mostrar anuncios, phishing y exposición de datos a otras aplicaciones. Gracias a su habilidad para abrir una URL en un navegador, el criminal detrás de este ataque puede generar páginas de phishing para diversas plataformas y abrirlas en un navegador. De esta forma, el cibercriminal lleva a cabo ataques de spear-phishing.

Por otra parte, debido a su habilidad para abrir aplicaciones en Google Play o 9Apps a través de una búsqueda mediante un determinada palabra clave o incluso en la propia página de la aplicación, el atacante puede aumentar sus beneficios ofreciendo acceso a otras potenciales amenazas. Asimismo, gracias a esto el atacante puede instalar una aplicación para uso en remoto desde un servidor asignado, pudiendo así instalar nuevos elementos de malware cuando sea necesario.

Las aplicaciones infectadas presentan una característica común: todas utilizan un Kit de Desarrollo de Software (en inglés, SDK) malicioso para llevar a cabo estas operaciones. Aunque existen SDKs cuyo objetivo es obtener rédito económico de las aplicaciones para móviles, los desarrolladores de videojuegos han elegido un SDK que les permite bombardear a los usuarios con una enorme cantidad de anuncios, lo que les permite aumentar sus ingresos.

Para contrarrestar los efectos que este tipo de amenazas provocan Check Point cuenta con SandBlast Mobile, la solución líder de defensa contra amenazas móviles avanzadas. Gracias a su infraestructura On-device Network Protection, Check Point ofrece prevención de amenazas en los dispositivos móviles

de la empresa que antes solo estaban disponibles en soluciones de seguridad de red y endpoints. Al revisar y controlar todo el tráfico de red del dispositivo, SandBlast Mobile evita los ataques de phishing en todas las aplicaciones, correo electrónico, SMS, iMessage y aplicaciones de mensajería instantánea. Además, esta solución evita el acceso a sitios web maliciosos o restringidos, y que los dispositivos infectados accedan a los recursos corporativos y se comuniquen con botnets. Para garantizar la privacidad de los usuarios y de sus datos, SandBlast Mobile valida el tráfico en el propio dispositivo sin enrutar los datos a través de un gateway corporativo.

Datos de contacto:
eVerythink PR

Nota de prensa publicada en: Madrid

Categorías: Juegos E-Commerce Software Ciberseguridad Dispositivos móviles